QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice)*
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
Joseph H. Margolies (admitted *pro hac vice*)
josephmargolies@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (CA Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Josef Ansorge (admitted *pro hac vice)*
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted pro hac vice)
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Counsel for Defendant Google LLC
Additional counsel on signature pages

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION

CHASOM BROWN, *et al.*, individually and on behalf of all similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

GOOGLE'S REPLY IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT

Hon. Yvonne Gonzalez Rogers
Courtroom: 1 – 4th Floor
Date: May 12, 2023
Time: 1:00 p.m.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

I. INTRODUCTION

Plaintiffs identify no evidence supporting their core claim: that Google "represented and by contract promised not to collect and use private browsing information while users were visiting non-Google websites and signed out of their Google accounts." SUF 1. The absence of that promise is made plain by the at-issue agreements and disclosures. Nor is there any genuine dispute that Google made no other promises or statements that might negate Plaintiffs' admitted consent to the data collection described in Google's Privacy Policy. SUF 4, 13–14. To the contrary, the disclosures clearly explain that PBM provides privacy in certain ways and not others, and the record confirms that PBM provides privacy *exactly* as Google described. The Court should grant summary judgment.

Recognizing that the cited disclosures do not make the promise alleged, Plaintiffs devote the lion's share of their opposition to arguing that the Court is *legally required* to accept Plaintiffs' position because Judge Koh's motion-to-dismiss decision is "law of the case." Opp. 5–7, 24. Not so. As the Court correctly explained when the *Calhoun* Plaintiffs made the same argument, "[a] ruling by a court for purposes of a motion to dismiss does not bind the court on a subsequent motion for summary judgment as the standards are entirely different: one considers plausibility, the other, the actual factual record."[1] *Calhoun v. Google*, 2022 WL 18107184, at *12 n.8 (N.D. Cal. Dec. 12, 2022). The Court should reject the argument here, too. Puffery is no substitute for proof.

Taking another page from the *Calhoun* Plaintiffs' playbook, Plaintiffs selectively quote internal Google emails and documents—many of which are unrelated to the at-issue disclosures or data collection. The cited documents relating to Incognito were largely written by a single Google employee concerned about the Incognito name and icon. *See* Resp. to Plaintiffs' Proposed Additional Facts ("PAF") at PAF 9, 12. But even these internal challenges characterize Google's Incognito

[1] Plaintiffs' reliance (Opp. 6) on *U.S.* v. *Alexander*, 106 F.3d 874, 876 (9th Cir. 1997) is misplaced. *Alexander* involved an evidentiary ruling in a criminal case submitted to the jury. The Ninth Circuit has since clarified that "*Alexander* applies only to cases in which a submission to the jury separates the two decisions"; by contrast, a district court is "free to reconsider its own prior ruling" where, as here, "the district court had neither been divested of jurisdiction nor submitted this case to the jury." *Robins v. Spokeo, Inc.*, 742 F.3d 409, 411 (9th Cir. 2014), *vacated and remanded on other grounds*, 578 U.S. 330 (2016); *U.S. v. Smith*, 389 F.3d 944, 950 (9th Cir. 2004) (distinguishing *Alexander* and explaining that "[t]he law of the case doctrine is 'wholly inapposite' to [the] circumstances" here).

disclosures as "admirably clear, concise, and accurate." *Id.* And those documents show, at most, that Google engaged in robust debate on how best to convey Incognito's privacy-enhancing functionality to its large and diverse user base. *See, e.g.*, PAF 7, 21. Regardless, Plaintiffs' cherry-picking and mischaracterizations of internal documents cannot save their claims because extrinsic evidence is irrelevant to the legal questions of whether Plaintiffs consented to the data collection (they did), and whether Google promised "not to collect or use private browsing information" (it did not).

II. ARGUMENT

A. Plaintiffs and Class Members Lack Article III Standing

Discovery has disproven Plaintiffs' core theory—that Google built "cradle-to-grave profiles" linking users' PBM data with their Google Accounts or identities. FAC ¶¶ 54, 69, 91–112. Plaintiffs admit Google does not do this, now arguing only that it would be "trivial" for it to do so. SUF 56. But even if such linking *were* trivial—and it is not[2]—Plaintiffs do not claim that Google does it. SUF 66. That is not *terra firma* for standing. The issue boils down to whether internet users suffer concrete injuries when web-service providers receive anonymous information indicating that an unidentified user visited a particular site or sites. *See* Mot. § II.A. They do not.

Standing for browsing data privacy claims may exist where the data is associated with users' identities. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (finding privacy interest in browsing data that Facebook "correlat[ed with] . . . users' personal Facebook profiles"); *cf. Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119 (9th Cir. 2020) (finding privacy interest in "individual private messages"). By contrast, the Ninth Circuit—and this Court—have found standing *lacking* where the information is "non-individually identifiable." *Cahen v. Toyota Motor*, 717 F. App'x 720 (9th Cir. 2017); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (Gonzalez Rogers, J.).[3] Simply stated, users are not "injured" merely because

[2] In the lengthy discovery process overseen by Magistrate Judge van Keulen and the Special Master, Google was *not* able to identify Plaintiffs' PBM data, other than in a controlled experiment that could not be replicated without the same knowledge, consent, and active participation of the user that Plaintiffs provided.

[3] Plaintiffs attempt to distinguish *I.C.* on the basis that it involved an "accidental data breach of non-private data" (Opp. 3 n.1), but the accidental nature of the breach is irrelevant because it goes to the defendant's intent, not the plaintiff's injury.

anonymous browsing data they generated during PBM sessions is collected or used.

Plaintiffs' assertion of statutory claims does not change the conclusion. *See* Opp. 3. Standing is not conferred automatically merely because a statute "arguably creates a 'substantive right.'" *Bassett v. ABM Parking Services, Inc.*, 883 F.3d 776 (9th Cir. 2018) (affirming dismissal of FCRA claim where there was no allegation that private information was disclosed). Plaintiffs still must "demonstrate how the 'specific' violation of [a statute] . . . actually harmed [them] or 'present[ed] a material risk of harm.'" *Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F3d 1166, 1174 (9th Cir. 2018) (affirming grant of summary judgment for lack of standing). They fail to do so.

Nor can the mere assertion of a breach of contract claim confer standing where there is no concrete injury. *See I.C.*, 600 F. Supp. 3d at 1045, 1054–55; *Svenson v. Google Inc.*, 2016 WL 8943301, at *10 (N.D. Cal. Dec. 21, 2016) ("a claim for nominal damages is insufficient to establish injury in fact for purposes of Article III"); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 990–91 (N.D. Cal. 2015) (Cal. Civ. Code "Section 3360 sets forth the rule that a plaintiff who has suffered an injury, but whose damages are speculative, is entitled to nominal damages . . . . But the statute does not relieve the plaintiff of proving injury.").

Alternatively, Plaintiffs argue for standing because "a jury could find that private browsing data *is* identifying." Opp. 3 (emphasis added). That is baseless. At most, the cited documents show that Google is *capable* of identifying PBM users—*if* it were to violate the policies and technical safeguards it put in place to prevent that from occurring. Plaintiffs' related argument (Opp. 4) that a jury could find that PBM data is identifying simply because data from signed-out users (including PBM users) may be stored "alongside" (but is not linked to) data from signed-in users, is also wrong. *See* PAF 4. That data from identified and unidentified users may be stored in the same location is irrelevant. It is undisputed that the signed-out and signed-in data are not linked.[4] This is plain from both the extensive record and absence of any evidence showing Google linked data from Plaintiffs'

[4] The rare exception, as Plaintiffs point out (SUF 63), is when Google is attempting to prevent fraud or criminal activity. But the policy document Plaintiffs cite for this point makes clear that the exception requires multiple levels of approval and may be invoked only in specific circumstances. Broome Ex. 71. Plaintiffs fail to identify any evidence that signed-out PBM data generated by them or any Class Members was ever identified pursuant to this exception.

PBM sessions to their Accounts, identities, or signed-in data. SUF 47–57, 59–60, 63–67.

Finally, Plaintiffs assert that, under *Facebook Tracking*, they have standing because they purportedly retain a "stake" in Google's "unjust enrichment." But the circumstances that gave rise to a "stake" in *Facebook Tracking* were "cradle-to-grave profiles" of "personally identifiable browsing history," 956 F.3d at 598–99, not the kind of orphaned islands of unidentified data here.

B. Each Claim Fails Because Plaintiffs and Class Members Expressly Consented to Google's Collection and Use of the Data

It is undisputed that Plaintiffs and Class Members are Google Account holders who each consented to Google's Privacy Policy when they created their Accounts. SUF 3–6. As this Court has held, the Privacy Policy discloses the collection and use of data that Plaintiffs challenge—*i.e.*, the data Google receives and uses for advertising, analytics, and other services when users visit a website using Google's services. *Calhoun*, 2022 WL 18107184, at *13–17. There is no ambiguity in these sections of the Privacy Policy. *See id.* The Court also found that the Privacy Policy applies to the challenged data collection irrespective of which browser the user chooses to employ. *Id.* at *10. The only remaining question in the consent analysis is whether Google represented that a particular browser *mode*—PBM—would *prevent* the data collection, thereby negating consent. The record shows it did not. Plaintiffs' repeated refrain that Google "represented [it] would not collect and use private browsing information" is pure *ipse dixit*.

Plaintiffs' efforts to distinguish *Calhoun* (Opp. 6) fail. The sections of the Privacy Policy describing the data Google receives from its services—via the same industry-standard HTTP requests at issue in *Calhoun*—do so in terms that necessarily are both browser- and *mode*-agnostic.[5] *See Calhoun*, 2022 WL 18107184, at *9–10; SUF 11, 18, 20. Indeed, prior to May 2018—when Plaintiffs consented to the Privacy Policy (SUF 5, 14)—it did not mention *any* specific browser modes. SUF 19. Thereafter, the Privacy Policy briefly references Incognito as a "private" mode, but nowhere suggests it prevents the data collection that it goes on to describe in plain language.

[5] Contrary to Plaintiffs' assertion that *Calhoun* is distinguishable because it involved only "*signed-in*, *regular* browsing data," Opp. 6, *Calhoun* also involved "signed-out" data received from users in Chrome's Basic and Guest modes. *Calhoun v. Google, LLC*, No. 20-CV-5146, Dkt. 429 at 2, 17. Regardless of mode, Google treats all signed-out data as "unauthenticated"; it is not categorized by whether the user is in PBM or another signed-out mode. *See* SUF 49.

As this Court correctly explained, "having Google's disclosures of the at-issue data in browser-agnostic terms, rather than by specific-browser, enables Google users, irrespective of the browser used, to know how it is that Google collects and utilizes one's data." *Calhoun*, 2022 WL 18107184, at *10 n.7. The same reasoning applies to browser *modes*. *See id.* (noting general data policies are important because browser functionality and settings vary and change over time). Irrespective of browser mode, the categories of data Google receives and the purposes for which it is used as described in the Privacy Policy remain the same.[6] SUF 7, 9, 11, 14.

In the face of their express consent to the data collection detailed in the Privacy Policy, Plaintiffs argue for an unworkably complex consent framework at odds with common sense and relevant authority. Opp. 9. Plaintiffs cite no case holding that, to obtain consent to data collection, companies must enumerate every mode, setting, or circumstance impacting—or *not* impacting—that data collection. This Court and the Ninth Circuit have both rejected this approach. *See Calhoun*, 2022 WL 18107184, at *13 (rejecting plaintiffs' argument that Google did not "explicitly notify" Chrome users that the data would be collected even if they did not use Chrome's sync mode); *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) (rejecting plaintiffs' argument that, "though they gave general consent to Facebook's data tracking and collection practices[,] they did not consent to collection of health related data due to its 'qualitatively different' and 'sensitive' nature"). Even under Plaintiffs' unworkable standard, describing the data collection in mode-specific terms would make little sense because Incognito *does not affect* the at-issue transmissions. Fact 9.

Because Plaintiffs' general consent to the data collection is not genuinely disputed, and they fail to identify any Google statement negating their consent, summary judgment should be granted.

C. Plaintiffs' and the Class's Claims Should Be Dismissed for Additional Reasons

1. Breach of Contract (Count 6)

(a) The Contract Does Not Make the Allegedly Breached Promise

"To claim breach of a written, integrated contract, a plaintiff must identify 'the specific

[6] As explained in the Motion, the key differences between Incognito and other Chrome modes (as Google explains elsewhere (*see* SUF 50–54, 57, 59)) are that Incognito automatically signs users out of their Google Accounts, blocks the sharing of existing cookies, and deletes new cookies, browsing history, and information entered in forms from the browser when the user closes the session.

provisions' imposing the obligation the defendant allegedly breached." *EM General, LLC v. Electronic Commerce, LLC*, 2021 WL 6618660, at *3 (N.D. Cal. Mar. 17, 2021) (Gonzalez Rogers, J.) (citing cases); *Ewert v. eBay, Inc.*, 602 F. App'x 357, 359 (9th Cir. 2015) (affirming dismissal of contract claim because plaintiffs "failed to identify a provision in the User Agreement that either expressly prohibited [the challenged action] or created an exception to the general rule set forth in the User Agreement that [defendant] could [take the challenged action]"). Plaintiffs fail to identify a specific contractual provision "promising" "that Google would not collect and use private browsing information."[7] Instead, they stitch together a patchwork of sentence fragments from various documents and ask the Court to *imply* that promise. The Court should deny their request. Indeed, even if such a promise *were* reasonably implied from the documents Plaintiffs cite, "'implicit duties' are insufficient to state a cause of action for breach of contract." *EM General*, 2021 WL 6618660, at *3; *see also Facebook Tracking*, 956 F.3d at 610 (affirming dismissal of contract claim because plaintiffs failed to identify "an explicit promise not to track logged out users"); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 982-83 (N.D. Cal. 2016) (dismissing contract claim based on alleged implicit duties). This alone defeats the contract claim as a matter of law.

Lacking a specific provision upon which to base their contract claim, Plaintiffs invite error by asking the Court to find the alleged contract is "reasonably susceptible" to their interpretation. Opp. 7. The Court could imply the promise alleged from the cited documents only by conflating distinctly defined terms (*i.e.* "Chrome" and "Google"), inserting words that do not appear, and contorting Google's statements to mean something obviously not intended. That is the *opposite* of how Courts interpret contracts under California law.[8]

[7] In fact, several of the documents on which Plaintiffs rely contain *no reference at all* to Incognito or PBM. These include Google's general Terms of Service ("TOS"), the Chrome and Chrome OS Additional TOS, and the pre-May 2018 Privacy Policy. *See* SUF 15–17, 19.

[8] Plaintiffs ask the Court to violate numerous bedrock principles of California contract law: (1) the contract must actually "express the obligation sued upon," *Anthem*, 162 F. Supp. 3d at 978 (quoting *Murphy v. Hartford Accident & Indem. Co.*, 177 Cal. App. 2d 539 (1960)); *Facebook Tracking*, 956 F.3d at 610 (allegedly breached promise must be "explicit"); (2) "'implicit duties' are insufficient to state a cause of action for breach of contract," *EM General, LLC,* 2021 WL 6618660, at *3; (3) a "simple failure to disclose a practice doesn't constitute breach of contract," *In re Facebook, Inc. Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019); and (4) "when courts construe an instrument, a judge is 'not to insert what has been omitted, or to omit what has been inserted,'" *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937, 954 (2008).

Plaintiffs' substantial reliance on the post-May 2018 Privacy Policy is a case in point. Plaintiffs assert that the Privacy Policy's description of Incognito as a private mode is a binding, contractual obligation that PBM provides *absolute* privacy *from Google*. But it does not say that. What that short, introductory paragraph does say—in plain language—is that Chrome's Incognito mode is one of numerous ways that users can manage their privacy when using Google services. SUF 20. And that is true—as even Plaintiffs' own privacy expert admits. SUF 75–81. Plaintiffs' purposefully myopic reading of Google's general disclosures[9] is belied by the rest of the same paragraph where the Privacy Policy describes other examples of privacy-enhancing functionality that nevertheless require sending information to Google. Ex. 100 ("manage your privacy" by "sign[ing] up for a Google Account if you want to . . . see more relevant search results" or "use many Google services when you're signed out" (in which case Google still receives data but it is not associated with an Account)). These examples each necessitate the communication of data to Google and illustrate that "private" cannot reasonably be construed to mean *absolute* privacy from Google. Similarly, it would be unjust to allow Google to be held liable for indisputably accurate statements simply because Plaintiffs allege they *inferred* from them something other than what they say.[10]

Finally, Plaintiffs imply the alleged promise based on their selective quotations of internal documents. That effort fails because Plaintiffs do not claim any specific terms are ambiguous, nor do they "tie [their] extrinsic evidence to specific terms," which is "essential." *Meisner v. JP Morgan Chase Bank, N.A.*, 2022 WL 837230, at *5 (E.D. Cal. Mar. 21, 2022) ("extrinsic evidence . . . must [] be tethered to specific contractual language"). Even if they had, the documents are not the kind of extrinsic evidence "regarding the drafting, negotiation, and performance of the" contract that courts

[9] The Privacy Policy "governs the collection of those categories of information identified by plaintiffs," *Calhoun*, 2022 WL 18107184, at *10, while the Chrome Notice (and documents linked to the Chrome Notice, like the Chrome Privacy Whitepaper) describe "features that are specific to Chrome," *id.* at *4, like Incognito mode. A statement in Google's general privacy policy that Incognito mode is one way users can manage their privacy therefore cannot override the Chrome Notice's specific explanation of how Incognito works.

[10] For example, Plaintiffs should not be permitted to hold Google liable for the Chrome Notice's statement that "You can limit the information *Chrome* stores on *your system* using incognito or guest mode," Opp. 13 (emphasis added), because it it is undisputed that Incognito *does* limit the information stored on users' systems, SUF 78, 81.

may consider. *See Travelers Indemnity Co. of Connecticut v. Premier Organics, Inc.*, 2017 WL 4355043, at *3 (N.D. Cal. Sept. 29, 2017) (Gonzalez Rogers, J.).

(b) Plaintiffs Base their Contract Claim on Non-Contractual Documents

Plaintiffs' contract claim should also be dismissed to the extent it is based on documents that are not contractual as a matter of law.[11] These include the Incognito Screen, the Search & browse privately Help page, and the post-March 2020 Privacy Policy.

The Incognito Screen: Plaintiffs claim the Incognito Screen is "incorporated by reference" in the Chrome Notice because the Chrome Notice references "Incognito *mode*." Opp. 7. That is not the law. The incorporation by reference doctrine requires, *inter alia*, that the reference to the incorporated document—and the fact that it is incorporated—be *clear and unequivocal*."[12] *Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997) (emphasis added); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 791 (N.D. Cal. 2019) ("the *reference* to the document [must] be *unequivocal*"). Indeed, even if the external document is "mention[ed]" in the contract, that "is not the same as specifically directing the parties' attention to the terms of the external document in a manner that could be construed as eliciting the parties' consent to its separate terms." *Amtower v. Photon Dynamics, Inc.*, 158 Cal. App. 4th 1608 (2008). Here, the alleged contract does not even "mention" the Incognito *Screen*. It mentions only the mode itself.

The Search & browse privately Help page: The Help page is not a standalone contract. *See Rodriguez v. Google LLC*, 2022 WL 214552, at *3 (N.D. Cal. Jan. 25, 2022) (Google Help page is not a standalone contract). Nor is it incorporated in the contract merely because it is hyperlinked to the post-May 2018 versions of the Privacy Policy. Chief Judge Seeborg correctly rejected this argument when Plaintiffs' counsel made it in *Rodriguez v. Google LLC*, 2021 WL 6621070, at *4

[11] Plaintiffs' alleged "contract" consists of three documents: the general TOS, the Chrome TOS, and the Chrome Notice. SUF 15. Plaintiffs allege these documents incorporate the Privacy Policy, the Search & browse privately Help page, and the Incognito Screen. *Id.*

[12] Plaintiffs read too much into *Shaw*'s use of the word "guide." That decision held that the parties' agreement incorporated the University's Patent Policy because: "The patent Agreement (1) directs Shaw to 'Please read the Patent Policy *on reverse side and above*,' and (2) states that, in signing the patent agreement, Shaw is 'not waiving any rights to a percentage of royalty payments received by University, as set forth in University Policy Regarding Patents." 58 Cal. App. 4th at 54 (emphasis added). This is the type of "clear and unequivocal" reference California law requires.

(N.D. Cal. Aug. 18, 2021) ("mere fact of a hyperlink" does not satisfy incorporation by reference doctrine).

The Post-March 2020 Privacy Policy: Nor can Plaintiffs support their contract claim with the Privacy Policy in effect when they filed suit. By then, "Google's Terms of Service explicitly excluded Google's Privacy Policy." *Calhoun*, 526 F. Supp. 605, 621 (N.D. Cal. 2021).

(c) Plaintiffs Rely on Statements that Are Not Enforceable "Promises"

Once the contract is properly defined by the Court (*supra* § II.C.1(b)), Plaintiffs are left to base their claim only upon the Privacy Policies in effect from June 2018–March 2020, and the Chrome Notice. But even the cited statements therein (*see* Opp. 13) are not enforceable "promises," because they merely provide "a general description of how [Google's] system works" and "contain no promissory language."[13] *See Block v. eBay*, 747 F.3d 1135 (9th Cir. 2014).

Plaintiffs argue that "Google errs by relying on cases addressing whether a document amounts to a contract in the first place." Opp. 13 (citing Mot. 15). That is wrong. The Ninth Circuit's *Block* decision—upon which Google primarily relies and which Plaintiffs ignore—analyzed the enforceability of statements in "eBay's User Agreement," a generally enforceable contract. Mot. 15–16 (citing *Block*). Indeed, in holding that the User Agreement clauses at issue were not enforceable, the Ninth Circuit "contrast[ed]" them with "other clauses in the agreement [that] contain explicit promissory language" and *were* enforceable. 747 F.3d at 1139. *Block* thus stands for the proposition that, even in a binding consumer agreement, a company can provide information about its products and services without creating contract liability. *Id.* This reasoning applies to every one of the "promises" Plaintiffs claim Google breached. *See* Opp. 10–11, 13; *see also* Mot. 7–8, 12–16.

2. Federal Wiretap Act Interception Claim (Count 1)

(a) Website Developers' Consent Defeats the Federal Wiretap Claims

The record confirms that websites consented to the at-issue data collection by installing Google's scripts *for the purpose of sending the data to Google* to provide desired services. SUF 90–97, 100–01. Neither of Plaintiffs' responses (Opp. 15–16) creates a triable issue.

[13] The same is true of the statements Plaintiffs cite in Search & browse privately page, and the Incognito Screen, in the event the Court finds those documents are contractual.

First, Plaintiffs can no longer rely on their pleadings. Discovery has shown that developers consented to the data collection regardless of browsing mode. SUF 92. Dr. Zervas analyzed information available to website developers (many of whom test their sites in PBM) and concluded that they incorporate Google's code knowing it functions the same in PBM. Ex. 80 ¶¶ 48–49. Among other examples, Google's public documentation for Analytics explains that "instances of incognito and private browsing[] are counted" in Analytics reports. *Id.* ¶ 95. Consistent with this evidence, the 25 web domains with the highest Google Analytics and Ad Manager traffic "all provided notices to users about data collection" that (1) display regardless of whether the user is in PBM, (2) often "includ[e] specific references to [use of] Google's services," and (3) do "not indicate or suggest that this data collection would stop when a user browses in [PBM]." *Id.* ¶¶ 85–89. In addition, Plaintiffs' experts and counsel continue using Google services on their *own* sites fully aware that the services function in PBM. SUF 92. They cannot create a triable issue as to developer consent on this record.[14]

Second, Plaintiffs' argument (Opp. 16) that Google represented it would comply with its own Privacy Policy is not evidence that developers did not consent to the data collection. The Privacy Policy has never represented that PBM blocks the data collection described therein. *Supra* § II.C.1(a), iii. And even if a *user* wrongly interpreted the Privacy Policy in the manner alleged, that is insufficient to negate the independent consent of *web developers*. *See Rodriguez v. Google LLC*, 2021 WL 2026726, at *5 (N.D. Cal. May 21, 2021) (rejecting identical argument).

Plaintiffs' invocation of the crime-tort exception (Opp. 16) is meritless. As Chief Judge Seeborg reaffirmed just this month, "the crime-tort exception[] require[s] . . . sufficient facts to show that 'the primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously,'" and "does not apply to a case such as this, where Defendant's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'" *Katz-Lacabe*

[14] Plaintiffs' claim that Google's evidence is "disputed" are illusory. *See* SUF 92. Messrs. Keegan and Hochman claim to have learned of the collection at issue through this case, but Mr. Keegan plainly consented anyway, Ex. 58 224:23–226:10, and Mr. Hochman admits that "I am a Google Analytics and Google Ads customer, and Google has not provided me with an option to ensure that its tracking and advertising code would avoid collecting data from private browsing sessions," Ex. 77 ¶ 136; *see also id.* App'x A ¶¶ 20–22 (Google's disclosures to website developers identify data collected "generally" and do not exclude private browsing data).

v. Oracle Am., Inc., 2023 WL 2838118, at *10 (N.D. Cal. Apr. 6, 2023) (quoting *Rodriguez*, 2021 WL 2026726, at *6 n.8); *see also* Mot. 17 n.15 (collecting cases). Plaintiffs proffer *no evidence* that Google's "primary motivation" was to injure them. And their allegation that Google "intercepted [their communications] for the purpose of associating their data with user profiles"—the only basis for Judge Koh's application of the crime-tort exception at the pleading stage, Dkt. 113 at 20, 22–23—has been thoroughly debunked.[15] *See* SUF 65–66.

(b) The Ordinary Course of Business Exception Applies

It is undisputed that Google code installed by website developers is the "device" causing users' browsers to send data to Google. SUF 91. Nor is there a genuine dispute that Google uses this code to provide ads and analytics services to websites choosing to use them—core components of Google's business. SUF 90, 93–97. That alone defeats their Wiretap claims. *See* Mot. 18–19.

Plaintiffs attack a strawman in arguing that Google has failed to demonstrate that "users would be unable to visit non-Google websites but for" the at-issue code. Opp. 17–18. That is not Google's argument, nor is it the law. Google need only show "some nexus between the need to engage in the alleged interception and the [defendant's] ultimate business." *Matera v. Google Inc.*, 2016 WL 8200619, at *14 (N.D. Cal. Aug. 12, 2016). That nexus is plainly present here.

Plaintiffs' alternative arguments are equally unavailing. The purported "evidence that Google uses the data for its own enrichment . . . separate and apart from any services it provides to websites," Opp. 18, actually shows that Google uses the data to enhance those same services. *See* PAF 26–27. Improving the services for which it collects the data in the first place—a practice Google discloses, *e.g.*, Ex. 93 at -22; *see also Calhoun*, 2022 WL 18107184, at *3–4 (quoting Privacy Policy)—is undeniably part of the ordinary course of its business.[16]

---

[15] Plaintiffs' reliance on Judge van Keulen's sanctions orders, which they brazenly mischaracterize, is also misplaced. The orders did *not* sanction Google for "hid[ing] how it uses private browsing data," *see* PAF 4, and expressly *rejected* Plaintiffs' request for an adverse inference. *See* Dkt. 898 at 12 (ruling the record "does not support an inference that the late-disclosed information was unfavorable to Google").

[16] *See Hammerling v. Google LLC*, 2022 WL 17365255, at *9 n.13 (N.D. Cal. Dec. 1, 2022) ("The provision of new, improved, and more personalized services is fundamentally compatible with, and largely indistinguishable from, Google's 'commercial purposes.'").

(c) There Is No Evidence that Google Intercepted the "Contents" of Plaintiffs' Communications

Plaintiffs' contention that "the specific webpage being viewed" and "other minute user interactions" are the "contents" of communications, Opp. 18, flatly ignores the Ninth Circuit's decision in *In re Zynga Privacy Litigation*, which holds that "HTTP referer information" including the "address [that] identifies the location of a webpage a user is viewing" is not "content." 750 F.3d 1098, 1105, 1107, 1109 (9th Cir. 2014). Nor are "minute user interactions" like keystrokes, mouse clicks, visit duration, and similar data.[17] *See* Mot. 20 & n.18 (collecting authority).

Although it may be true that "[u]nder some circumstances, a user's request to a search engine for specific information could constitute a communication," *Zynga*, 750 F.3d at 1108, Plaintiffs proffer no evidence that Google collected search terms from them in PBM. The URL containing search terms in Plaintiffs' brief (Opp. 19) was generated for litigation by Plaintiffs' expert. PAF 34. The other URLs Plaintiffs cite were likewise generated under experimental conditions, and captured on Plaintiffs' browsers rather than from Google's servers. PAF 33. None is a basis for liability.

3. Cal. Penal Code §§ 631 & 632 ("CIPA") (Count 2)

Plaintiffs' failure to offer evidence that Google collected the "content" of their communications is similarly fatal to their CIPA § 631 claim. *See* Mot. 20. And their § 632 claim fails because they do not identify any evidence that their "communications" were confidential within CIPA's definition. Plaintiffs quote the first half of the definition of "confidential communication," Opp. 20, but conspicuously omit the second, which "excludes a communication made . . . in any [] circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c). That exclusion is dispositive—Plaintiffs admit they knew their browsing activity would be visible to third parties.

[17] In arguing that URLs constitute "content," Plaintiffs resort to mischaracterizing authority. *See* Opp. 19. The Ninth Circuit expressly held that *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) does *not* support classifying URLs as "content." *Zynga*, 750 F.3d at 1108. In *In re Google RTB Consumer Privacy Litigation*, this Court held (at the pleading stage) that plaintiffs sufficiently alleged content not based on URLs *alone*, but rather in combination with at least six other data categories. 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) (Gonzalez Rogers, J.). And the court in *In re Meta Pixel Healthcare Litigation* held only that URLs may be content when they contain "*the query string*" (*i.e.*, search terms). 2022 WL 17869218, at *11 & n.10 (N.D. Cal. Dec. 22, 2022).

SUF 98. It is immaterial that they allegedly did not expect Google to be among them. *Rodriguez*, 2021 WL 2026726, at *7 (expectation that Google would not record communications "does not reasonably give rise to the expectation that *nobody* (including [] developers) would").

4. California Penal Code § 502(c)(2) ("CDAFA") (Count 3)

Plaintiffs proffer no evidence that Google "accessed" their computers or did so "without permission," the core of a CDAFA violation. *Developers* choose to include the at-issue code as a component of their own websites, and browsers receive that code *only after requesting* the sites' full HTML code. SUF 90–97, 100–01; PAF 29. Plaintiffs cite no case applying CDAFA to that process, and no wonder: their interpretation would criminalize fundamental internet transmissions. *See* Mot. 22. Separately, CDAFA requires that the defendant "circumvent[] technical or code-based barriers," or otherwise "render ineffective any barriers . . . to prevent access." *Brodsky v. Apple Inc.*, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019). It is undisputed that PBM is no such barrier, *see* SUF 68–72, and Plaintiffs' only contrary argument is contractual, not technical. *See Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (plaintiff cannot show "access . . . without permission simply because [defendant allegedly] violated a contractual term of use").

Nor do Plaintiffs identify evidence of "damage or loss." They cannot meet CDAFA's "narrow conception of 'loss'" based on the theoretical value of data that "they might have received from commodifying" it. *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262 (9th Cir. 2019); *see also* Mot. 22–23 (collecting cases).[18] Plaintiffs mistakenly rely (Opp. 21-22) on *Facebook Tracking*, which held only that allegations of unjust enrichment were sufficient at the pleading stage *to confer standing* under the facts alleged in that case, not to support liability. 956 F.3d at 600–01; *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1038 (N.D. Cal. 2014) ("The requirements to allege standing are not the same as the requirements to plead injury under the substantive law.").

[18] *Andrews* concerned a claim under CFAA, CDAFA's federal equivalent. Apart from CFAA's $5,000 minimum damages requirement, the CFAA and CDAFA analyses are materially identical. *See Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020).

5. Invasion of Privacy and Intrusion Upon Seclusion (Counts 4 and 5)

Plaintiffs fail to raise genuine disputes on either element of their privacy claims—(1) a reasonable expectation of privacy, and (2) a highly offensive intrusion. *Facebook Tracking*, 956 F.3d at 601. *First*, the at-issue data was "private" because Google undisputedly did not link it to their identities. SUF 62–67. Any expectation of *additional* privacy beyond that specifically described in Google's disclosures was unreasonable. *See Sanchez v. L.A. Dep't of Transp.*, 2021 WL 1220690, at *3 (C.D. Cal. Feb. 23, 2021) (no reasonable expectation of privacy in unidentified data even if de-anonymization is possible); Mot. 23 n.22. Plaintiffs' claim that *Facebook Tracking* "soundly rejected" this argument (Opp. 22) is wrong because, unlike Google, Facebook allegedly made "*affirmative* statements that it would not receive information from third-party websites after users had logged out" and then "correlat[ed] users' browsing history with [their] personal Facebook profiles." 956 F.3d at 599, 602–03.

Second, Plaintiffs cannot show that Google's data collection and use was "highly offensive." Courts routinely reject privacy claims based on browsing and similar data because such "routine commercial behavior" is not highly offensive as a matter of law. *See* Mot. 23–24 & n.23 (collecting cases). That is particularly true where, as here, the data is unidentified. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1091 & n.11 (N.D. Cal. 2022) (alleged intrusion not "highly offensive" where information was anonymized). Plaintiffs argue the conduct is offensive because Google purportedly "knew it was deceiving users." Opp. 23. But the cited evidence does not support this conclusion. PAF 7, 12. Plaintiffs' decision to continue subjecting themselves to the alleged harm also precludes a finding of highly offensive conduct, notwithstanding their convenient "explanation" that they took no additional precautions because they are "in the middle of a lawsuit." SUF 105.

6. Unfair Competition Law ("UCL") (Count 7)

(a) Plaintiffs Fail to Establish UCL Standing

Plaintiffs' UCL claim should be dismissed because they fail to show they "lost money or property." Cal. Bus. & Prof. Code § 17204; Mot. 24–25. Plaintiffs' assertion that "there is a 'cash value' for data and 'an active market for data'" (Opp. 24), is neither sufficient nor supported by the

evidence. Under that theory, Plaintiffs would need to show not only that there exists a market for the data, but also an impairment of their ability to participate in the market. *Ji v. Naver Corp.*, 2022 WL 4624898, at *9 (N.D. Cal. Sept. 30, 2022). They show neither.[19] SUF 104; *see also Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022) (dismissing UCL claim because plaintiffs "did not allege they ever attempted or intended to . . . derive economic value from their PII" or that a "prospective purchaser of their PII . . . might insist on less favorable terms" due to defendant's conduct); *Facebook User Profile Litig.*, 402 F. Supp. 3d at 803–04 ("that Facebook may have gained money through its sharing or use of the plaintiffs' information…[is] different from saying the plaintiffs lost money"). Plaintiffs' assertion that their UCL standing arguments are "neither new nor novel" and are part of a "growing trend," Opp. 24 n.25, is simply wrong.[20]

(b) Plaintiffs Have an Adequate Remedy at Law

The law is clear that a party's assertion of legal claims—*e.g.*, breach of contract—bars a UCL claim for equitable relief. Mot. 25 & n.26 (citing authority). Plaintiffs fail to grapple with that authority and misapprehend the key question, arguing that "[m]onetary damages would only address Google's past conduct." Opp. 25. That argument has been consistently rejected. *See* Mot. 25 & n.25; *In re MacBook Keyboard Litigation*, 2020 WL 6047253, at *3 (N.D. Cal. Oct. 13, 2020) (fact that alleged injury is "continuing" does not mean legal remedy is inadequate).

III. CONCLUSION

For the foregoing reasons, summary judgment should be granted.

[19] The only evidence Plaintiffs' cite relates to (1) the value of private browsing data to Google or other digital advertisers, *see, e.g.*, Mao Ex. 25 § 7 (discussing financial impact to Google), Broome Ex. 75 § 4 (discussing online advertising revenue); (2) the value of *different* data to study participants, Mao Ex. 25 § 8 (discussing payments for participation in a panel that collects a wide range of data linked to the participant's identity); or (3) Plaintiffs' awareness of marketplaces for some types of browsing data which Plaintiffs never participated in, Mao Exs. 3–7.

[20] To the contrary, "[t]he weight of the authority in the district and the state . . . point in the opposite direction [of *Calhoun*]: that 'the "mere misappropriation of personal information" does not establish compensable damages.'" *Katz-Lacabe*, 2023 WL 2838118, at *8 (Seeborg, C.J.) (collecting cases).

DATED: April 26, 2023

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By: /s/ Andrew H. Schapiro
Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
Joseph H. Margolies (admitted *pro hac vice*)
josephmargolies@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (CA Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice*)
carlspilly@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jomaire A. Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
D. Seth Fortenbery (admitted *pro hac vice*)
sethfortenbery@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC